dHealth 2019 – From eHealth to dHealth
D. Hayn et al. (Eds.)
© 2019 The authors, AIT Austrian Institute of Technology and IOS Press.
This article is published online with Open Access by IOS Press and distributed under the terms
of the Creative Commons Attribution Non-Commercial License 4.0 (CC BY-NC 4.0).
doi:10.3233/978-1-61499-971-3-202

Performance of Hospitals in Protecting the Confidentiality and Information Security of Patients in Health Information Departments

Abbas SHEIKHTAHERI[a], Nasim HASHEMI[b,1] and Niyoosha-sadat HASHEMI[c]
[a]*Health Management and Economics Research Center, School of Health Management and Information Sciences, Iran University of Medical Sciences, Tehran, Iran*
[b]*Iranian Social Security Organization, Tehran, Iran*
[c]*Student, Islamic Azad University, Tehran North Branch, Tehran, Iran*

Abstract. Keeping health information confidential is an important aspect of managing health information. This study aimed at determining the performance of health information management departments (HIMD) to identify the policies of these hospitals, their similarities, and differences in their procedures in this respect. Managers of the departments and information disclosure and medical record staff in 22 teaching hospitals were invited to complete a questionnaire regarding their practices in four axes including confidentiality principles, principles of disclosure consent, disclosure information to external and internal users. We found that there are no specific national framework and guidelines for the disclosure of health information. Hospitals are undertaking different ways in this regard. In most cases, patients' consent is not considered necessary for disclosure and only hospital managers' or physicians' consent is sufficient.

Keywords: health information, privacy, security, confidentiality

1. Introduction

Since health data is sensitive and private, the need for confidentiality and security of these data is obvious [1-3]. Confidentiality refers to the protection of information against unauthorized access or disclosure and keeping information confidential should be conducted by controlling the access level of individuals (authorized users) in organizations, as well as protecting information at the time of data transmission [4-6]. Therefore, one of the most important responsibilities of the Health Information Management Departments (HIMD) in hospitals is compliance with the principles of confidentiality and information security [7]. The HIMDs should play a significant role in monitoring and observing laws, adhering to professional standards, and conducting appropriate procedures for keeping health information secure and confidential [5,8]. However, research conducted in different countries indicates the high deviations of the HIMDs with these principles [8], and notwithstanding, different countries have

[1] Corresponding Author: Nasim Hashemi, Iranian Social Security Organization, Tehran, Iran, E-Mail: Hashemi.nasim@tamin.ir

different policies and procedures to protect the privacy and security of patient information in hospitals [4]. For example, USA [9], Canada [10] and Australia [11] have enacted regulations in this regard. Furthermore, the European Union enacted the General Data Protection Regulation for protecting data and privacy for all individuals within the European Union (EU) and the European Economic Area (EEA) in 2016 [12]. In Iran, there is no clear policy to maintain the security and confidentiality of patient information. Some studies have shown that the confidentiality of medical records was not observed appropriately [6, 7]. Additionally, some previous studies indicated that patients are concern in this regard [13]. Considering the importance of the observance of confidentiality rules, this study carried out to determine the performance of HIMDs in teaching hospitals in Iran to identify their similarities and differences as a basis for compiling the policies of confidentiality and security of health information.

2. Method

This cross-sectional study was undertaken in 2018 in 22 teaching hospitals in Tehran, Iran. All of the managers of HIMDs, information disclosure and medical record officers (N=71) were invited and finally, 53 questionnaires were returned and analyzed. A questionnaire (32 questions) was developed based ona different scenarios and possible actions. Six questions were related to the demographic data and 24 questions were related to the principles of compliance with the confidentiality, compliance with the principles of information disclosure consent, and compliance with the principles of confidentiality in responding to internal and external users. In each question, the participants were asked to determine their practices in each case. Answer options for each question were defined based on possible actions. Respondents could choose more than one option or mention other procedures used in their hospitals. The validity of the questionnaire was determined based on the opinions of experts in health information management. Reliability was tested through test-retest (r=0.8). In order to collect data, paper-based questionnaires were distributed to participants. The participants were provided with the necessary explanations and time to complete the questionnaire. Data were analyzed by frequency and percentage of each actions using SPSS version 22.

3. Results

Most participants were women (89.3%), had a bachelor's degree (85.7%) and were specialists in the field of HIM (96.4%). The mean age of participants was 39.7 years and the average working experience was 16.5 years. In most hospitals (Table 1), patients do not have the right to review and request correction of their medical records (66%) and most of them do not release patients' information to them (47.1%). Most hospitals receive an obligation from the users for not disclosing the contents of the medical records (43.4%). Regarding the compliance with the principles of information disclosure consent (Table 2), we found that obtaining permission from the hospital administrators and authorities to disclose patient information without the patient's consent (67.9%), and access of the hospital doctors to the medical records without the patients' consent and only upon request from the doctor (56.6%) were considered adequate. Disclosure of any information requested by the users without the consent of

patients (43.4%) and disclosure of patients' information to their workplace and employers with only the permission of the hospital authorities and without the patients' consent (52.8%) were the most common processes in these hospitals.

Table 1. Compliance with the confidentiality principles of health information in HIMDs

Questions	Possible policies and procedures	Frequency (percentage)
Ownership of medical records	For the hospital	40(75.5)
	For the Patients	-
	For patients and the hospital	13(24.5)
Ownership of the information recorded in the medical records (not the physical records)	For the hospital	12(22.6)
	For the patients	2(3.7)
	For patients and the hospital	39(73.5)
Confidentiality notice and alerts to medical record users	Receive users' commitment to not disclose information	23(43.4)
	Oral reminder to prevent disclosure of information	21(39.6)
	No oral or written notice	4(7.5)
	Other	5(9.4)
Patient`s right to review and apply for his/her record correction	The patient has the right to review and apply for his/her documents	-
	Not at all allowed	35(66)
	Only with doctor's permission is allowed	13(24.5)
	Other	5(9.4)
The conditions for receiving patient information by the patient in the harmful conditions	The information is provided to the appropriate person as identified by the patient	17(32.1)
	The hospital doctor reviews the medical record to disclose the information	6(11.3)
	Information is disclosed in such a way as to minimize the harmful effects on the patient	-
	Information is not disclosed to the patient at all	25(47.1)
	Other	4(7.5)
Measures to disclose information in legal cases	Checking the signature of a patient by signing a consent letter	6(11.3)
	Writing a report by patient's doctor	27(50.9)
	Attaching the leaflet contains the hospital logo to the report	2(3.7)
	Other	10(16.9)

Regarding the external users (Table 3), responding to the legal requests with the order of the hospital director (88.6%) and providing medical records to other hospitals and external doctors with the orders of the hospital managers without patients' consent was 81.1%. Only 64.3% of participants stated that their hospitals had a policy for using medical records by the researchers. Disclosure of medical record information for

lawyers and the authorities only by the judiciary order was only 62.6%. Regarding the internal users (Table 4), we found that heads and managers of hospitals have convenient and fast access to medical records without the patients' consent (58.4%). Only 52.8% of participants declared that they had a clear policy for the use of patients' information in the educational programs.

Table 2. Compliance with principles of disclosure consent in HIMDs

Questions	Possible policies and procedures	Frequency (percentage)
Consent to release medical record information to applicants	Consent is received from patient	17(32.1)
	No consent is received from patient	2(3.7)
	The doctor`s permission is sufficient	8(15.1)
	The permission and orders of the hospital managers and authorities are sufficient	36(67.9)
The access of the hospital doctors to medical records	Without the permission of the patient and only upon the request from the doctor	30(56.6)
	Only with the written consent of the patient	4(7.5)
	Only with the permission of the hospital manager	15(28.3)
	Other	9(17)
Disclosure of medical records for the hospital where the patient is being transferred	With the consent of the patient	13(24.5)
	With the consent of the doctor	27(50.9)
	Without any consent form	8(15.1)
	Other	5(9.4)
Authorized information for disclosure without the consent of the patient	Patient's name, date of reception and patient's general condition	11(20.7)
	Results of experiments, x-rays, and electrocardiogram	6(11.3)
	The current physical and psychological history of the patient	8(15.1)
	Any kind of information that the applicant asks	23(43.4)
Conditions for providing patient information to their workplace	Only with the consent and request of patient	11(20.7)
	Just by asking the patient's workplace	11(20.7)
	Authorization of hospital authorities is sufficient	28(52.8)
	Other	3(5.7)

Table 3. Compliance with confidentiality principles in responding to external users in the HIMDs

Questions	Possible policies and procedures	Frequency (percentage)
The manner of getting medical records out of hospital	It can be taken out of the hospital	-
	It cannot be taken out of hospital	13(24.5)
	With request of judicial authorities, it can be taken out of hospital	39(73.5)
	It can be taken out of hospital to get a copy of pages	1(1.8)

Table 3. Continued

Questions	Possible policies and procedures	Frequency (percentage)
The access of other healthcare professionals outside the hospital to patient information	With the request of professionals	28(52.8)
	With written patients' consent	7(13.2)
	With permission of hospital directors	30(56.6)
	Other	6(11.3)
Guideline for researchers to use medical records	It is clear	33(62.3)
	Not specified	10(18.9)
	I do not know	10(18.9)
The requirements for providing medical records to other hospitals and external doctors	The requested information is provided to the applicant	2(3.7)
	Only with patient permission	10(18.9)
	With the orders of authorities and hospital directors	43(81.1)
	Other	5(9.4)
The circumstances required for providing medical records to insurance companies	Information is disclosed without patient's consent	7(13.2)
	Only with patient's consent	13(24.5)
	With the order of the hospital director	37(69.8)
Conditions for responding to requests from external agencies and offices	Positive response without patient`s consent	5(9.4)
	With the order of the hospital directors	47(88.6)
	With the patient's consent	6(11.3)
	Other	1(1.9)
The requirement for disclosure of medical records to lawyers and legal authorities	Consent or authorization is not needed	6(11.3)
	Only with patient's consent	7(13.2)
	Only by judicial decisions	33(62.6)
	Other	11(20.7)
The requirement for getting the patient's information by the patient him/herself	Patient has the right to receive his/her complete information	15(28.3)
	Patient does not have the right to receive his/her complete information	5(9.4)
	Only with the approval of physician, patient has the right to receive his information	7(13.2)
	Only with the approval of the authorities and the hospital directors, patients have the right to receive his/her information	26(49.1)
The conditions for receiving a copy of the records by the patient him/herself	He/she does not have the right to receive any copy at all	2(3.7)
	He/she can take copies of medical records	28(52.8)
	He/she can only receive the copies by the approval of the physicians	4(7.5)
	He can only receive the copies by the permission of the hospital directors	24(45.2)
	Other	4(7.5)

Table 4. Compliance with confidentiality principles in responding to internal users

Questions	Possible policies and procedures	Frequency (percentage)
Hospital authorities access (hospital head and director) to patients' medical records	They can easily access the information	31(58.4)
	Not allowed to access information	7(13.2)
	Only with the patient permission, they have the right to access the records	4(7.5)
	Other	13(24.5)
Hospital staff access to patients' medical records	Their access is in accordance with their personal responsibility and authority in order to do hospital affairs	34(64.1)
	If requested, they can access records	2(3.7)
	They have access only with the permission of the patient's physician	7(13.2)
	Other	10(18.8)
The use of medical records to assess the quality of health care	Only with the patient's consent	6(11.3)
	With the permission of the doctor	19(35.8)
	With hospital managers' permission	32(60.4)
	Other	6(11.3)
The presence of a clear policy for using patients' information in hospital educational programs	The hospital has specific policies	28(52.8)
	There are no specific policies	4(7.5)
	Hospital uses records at any time for training	17(32.1)
	Other	4(7.5)

4. Discussion

In general, the findings show that these hospitals, in some cases, use the same procedures, but in many cases, the current process of hospitals regarding the confidentiality and disclosure of information in different circumstances is not the same. Furthermore, in many cases, procedures of hospitals show that confidentiality and security of health information is not a priority, and they provide access to patients' information without their consents.

In the first axis, most hospitals take obligation from the users not to disclose information. In addition, in most hospitals, patients have no right to review and request correction of his/her information, and if the information is harmful, no information is given to patients. In the case that the information provided under legal conditions, a few hospitals controlled patients' consent and were mostly confined to the doctor`s report or the hospital's director order. Few hospitals stated that if a patient requests information from his/her records, he/she has access to this information with his/her identification card. Furthermore, in a small number of hospitals, keeping the confidentiality and privacy of patients was mentioned in the staff job descriptions. Some hospitals only gave the possibility to correct patients' identification data.

Additionally, it was found that in most hospitals, the doctors' access to patients' information is possible without the permission of patients and only by a doctor's request. For other users of the medical records, the permission of the hospital managers and authorities is considered sufficient. In most cases, the disclosure of information to the hospitals where a patient is transmitted is undertaken only with the physicians'

permission. In most hospitals, sending information to users did not require patients' consent. In addition, it was determined that hospital managers have access to patients' information without their consents, but other staffs have access to information only within their scope of tasks. The use of medical records to assess the quality of health care is also possible with the permission of the doctor. To send out information outside the hospitals, most hospitals do not receive consent from the patients and only the permission of the hospital authorities is considered sufficient, except in legal cases where the information is sent out merely by a request from the judicial authorities.

According to the HIPAA Privacy Policy, a patient has the right to access and control his health information [9]. According to Canadian law, health care providers and centers are required to protect personal information and to justify them about all information activities they carry out. Healthcare organizations should provide patients with access to their health information [10]. In Australia, there are laws developed to protect the privacy of health information for patients to access their health information [11]. General Data Protection Regulation has developed a framework for data privacy, rights of data subjects, and transfer of data for European countries [12] but in Iran it seems that hospitals do not have a common framework to protect health information privacy and give enough patients' access to their information and patients cannot control their information.

According to the HIPAA, patients' health information should not be released without their consent unless there is a clear reason for it; and users should also protect it. The patients should also be informed about what information is disclosed and for whom and why [9]. However, the findings showed that in Iran, a patient's consent to deliver the information is not taken into consideration, and therefore, patients do not have control over who has access to and uses their information. Moreover, the use of health information is allowed when it is permitted or required by the law, and the patient has expressed his/her consent to this disclosure [14].

Use of information to achieve the primary purposes of health information collection and other purposes such as planning, providing healthcare services, allocating resources, managing errors and risks, and improving the quality of care, training of health care providers is allowed without patients' consent, unless they have expressly announced their disagreement for this [15]. This issue is partly observed in Iranian hospitals. Application of health information for research, evaluation of healthcare quality and education do not dependent on patients' consent. Although the educational use of information is permitted [16,17], but the identity of patients should not be released [18] and students should be responsible for maintaining health information [19].

In the case of research, the written consent of patients is required unless based on the ethics committee, written consent of patients is not required or researchers use a limited set of data without the patient's identification data [20]. In other words, if the study needs identity information, the approval of the ethics committee should be available [21]. In some cases, such as health and medical research that benefits the community, and there is no possibility of obtaining consent from patients, instead of the consent form, appropriate mechanisms should be taken into account to protect the privacy of health information [22]. In Iranian hospitals, researchers are allowed to access the information with the permission of hospital managers, and researchers should have the ethics committee permission. Therefore, this issue is respected in our hospitals.

In summary, this study showed that in our country, there are no specific national frameworks and guidelines for the disclosure of health information and their privacy and security, and hospitals are conducting different ways in this regard. Also, in many cases, international principles are not respected. Therefore, a specific framework for security and confidentiality of health information may be developed in order to protect the confidentiality and security of health information in both electronic and manual medical record systems.

References

[1] G.S. Poduri, Confidentiality and patient records. *AP Journal of Psychological Medicine*. **14**(2) (2013),110- 113.

[2] N. Hajrahimi, S.M. Hejazi Dehaghani, A. Sheikhtaheri, Health information security: A Case study of three selected medical centers in Iran. *Acta Informatica Medica*. **21**(1) (2013), 42-45.

[3] J.R. Junges, M. Recktenwald, H.D Raymundo, et al. Confidentiality and privacy of information about patients treated by primary health care teams: a review. *Revista Bioética.* **23**(1) (2015), 200-206.

[4] T. NaseriBooriAbad, A. Sheikhtaheri. Information privacy and pervasive health: Frameworks at a glance. *Journal of Biomedical Physics* and *Engineering.* (2019), In press.

[5] M. Langarizadeh, A. Orooji, A. Sheikhtaheri, Effectiveness of Anonymization methods in preserving patients' privacy: a systematic literature review. *Studies in Health Technology and Informatics*. **248** (2018), 80-87.

[6] E. Mehraeen, H. Ayatollahi, M. Ahmadi, A Study of information security in hospital information systems, *Health Information Management*. **10**(6) (2014), 779-788.

[7] A. Hajavi, M. Khoushgam, M. Hatami, A Comparative study on regarding rate of the privacy principles in legal issues by WHO manual at teaching hospitals. *Journal of Health Administration*. **33**(11) (2007), 7-16.

[8] M. Farzandipour, Policies for providing medical records at hospitals. Dissertation of Health Information Management. (2002).

[9] K.A. Wager, F.W. Lee, J.P. Glaser, Health care information systems: a practical approach for health care management. John Wiley & Sons (2017).

[10] A. Thorogood, Protecting the privacy of Canadians' health information in the cloud. Can J Law Technol. 14 (2016), 173-213.

[11] New South Wales information and privacy commission, health records and information privacy Act 2002.

[12] General Data Protection Regulation (GDPR). (2016) Available from: https://gdpr-info.eu/

[13] A. Sheikhtaheri, M.S Jabali, Z.H. Dehaghi. Nurses' knowledge and performance of the patients' bill of rights. Nursing Ethics. **23**(8) (2016), 866-876.

[14] Government of Newfoundland and Labrador: Department of Health and Community Services, The personal health information act policy development manual. (2011).

[15] Personal Health Information Protection Act. (2004) Available from: https://www.ontario.ca/laws/statute/04p03.

[16] Uconn Health. Policy: Use of protected health information (phi) in education (POLICY NUMBER 2014-07). (2014) Available from: https://health.uconn.edu/policies/wp-content/uploads/sites/28/2015/07/policy_2014_07.pdf.

[17] UT Health HIPAA compliance program: Office of regulatory affairs and compliance: Using protected health information (PHI) for education. (2014).

[18] M. Abdelhak, S. Grostick, M.A. Hanken, Health Information: Management of a Strategic resource. Elsevier Health Sciences, (2014).

[19] University of Hawaii HIPAA training program, Appropriate uses of protected health information for educational purposes. (2014).

[20] UCI Office of Research. Protected Health Information (HIPAA). (2015) Available from: http://www.research.uci.edu/compliance/human-research-protections/researchers/protected-health-information-hipaa.html.

[21] Office of the Information and Privacy Commissioner, The health information Act: use and disclosure of health information for research.

[22] C. O'Keefe, D. Rubin, Individual privacy versus public good: Protecting confidentiality in health research. *Statistics in Medicine*. **34**(23) (2015), 3081-3103.